UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/759,402	01/12/2001	George Cybenko	389522	1647

30955 7590 05/16/2006

LATHROP & GAGE LC
4845 PEARL EAST CIRCLE
SUITE 300
BOULDER, CO 80301

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 05/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/759,402	CYBENKO, GEORGE	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the arguments filed on 28 February 2006.

2. Claims 1-16 are pending in the application.

3. Claims 1-16 have been rejected.

Response to Arguments

4. Applicant's arguments filed 28 February 2006 have been fully considered but they are not persuasive.

On page 4, the applicant argues that Ulyanov does not disclose encoding a program as a unitary matrix with n rows and n columns.

The examiner respectfully disagrees. Ulyanov does teach encoding a program into a unitary matrix. The program is encoded into unitary matrix Uf. The examiner asserts that a matrix is going to contain n rows and no columns.

On page 5, the applicant argues that because Ulyanov fails to teach encoding an input data string to a general program as a vector of length n, in the context of encryption, as required in claims 1 and 15.

The examiner respectfully disagrees. Ulyanov teaches that a program is encoded, as described above. The output of encoded program is a set of basis vectors (i.e. vectors 805). The examiner asserts that the vector will have a length. The reference reads upon having a vector of length n.

On page 5, the applicant argues that Ulyanov does not teach encoding a program, especially as a step in a method for encrypting a program. The applicant argues that Ulyanov

cannot teach loading such an encoded program and such an encoded string (with/on) a host computer.

The examiner respectfully disagrees. Ulyanov teaches encoding a program, as described above. The encoded program is loaded upon a host computer as an encoded string, as shown in figure 7.

On page 5, the applicant argues that Ulyanov does not teach "executing an encoded program, using the encoded data string, on the host computer".

The examiner respectfully disagrees. Ulyanov teaches executing the encoded program, in its encoded data string form, in order to decode the program. This all takes place on the host computer.

On page 6, the applicant argues that Ulyanov does not teach communicating results from a host computer to a network.

The examiner respectfully disagrees. Ulyanov teaches forwarding the result of the encoded programs to the other quantum computers.

On page 6, the applicant argues that Ulyanov does not teach decoding results into output representative of executing the program with the data string, wherein computations and data associated with the program and data string are unintelligible and useless at the host computer.

The examiner respectfully disagrees. Figure 8 of Ulyanov shows decoding of the encoded program. Once the encoded program has been forwarded from the host computer, the results become useless to this device. They are only discernible to the received device.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Ulyanov U.S. Patent No. 6,578,018 B1.

As to claims 1 and 15, Ulyanov discloses a method for encrypting programs for encrypted execution on a network having a remote host computer, comprising the steps of:

encoding a program as a unitary matrix with n rows and n columns [column 13 line 61 to column 14 line 6];

encoding an input data string to the program as a vector of length n, wherein execution of the program on the input data string is realized by matrix multiplication of the unitary matrix with the vector [column 16 line 1 to column 17 line 67];

loading the encoded program and the encoded data string on the host computer [column 16 line 1 to column 17 line 67];

executing the encoded program, using the encoded data string, on the host computer [column 16 line 1 to column 17 line 67];

communicating results from the host computer to the network [column 16 line 1 to column 17 line 67]; and

decoding the results into output representative of executing the program with the data string, wherein computations and data associated with the program and data string are unintelligible and useless at the host computer [column 15, lines 46-52].

As to claim 2, Ulyanov discloses that the step of encoding a program comprises converting the program to a unitary matrix multiplication [column 16 line 1 to column 17 line 67].

As to claim 3, Ulyanov discloses that the step of converting the program comprises converting the program to a unitary matrix multiplication U such that $U \varepsilon U_n$ for some integer n, where U_n represents a group of unitary matrices of size n [column 19 line 1 to column 20 line 44].

As to claim 4, Ulyanov discloses that the step of encoding the program comprises generating two independent identically distributed unitary matrices X, Y from the uniform probability distribution over U_n determined by the Haar distribution [column 16 line 1 to column 17 line 67].

As to claim 5, Ulyanov discloses that the step of encoding a program comprises the steps of computing U' as XUY* and communicating U' to the remote host computer over the network [column 16 line 1 to column 17 line 67].

As to claim 6, Ulyanov discloses that the step of encoding the input data string comprises converting the input data string to a vector b [column 16 line 1 to column 17 line 67].

As to claim 7, Ulyanov discloses that the step of encoding comprises the steps of computing b' as Yb and communicating b' to the remote host over the network [column 16 line 1 to column 17 line 67].

As to claim 8, Ulyanov discloses that the step of executing the encoded program, using the encoded data string, on the: host computer comprises the steps of computing the product of XUY* and Yb and communicating results to the network [column 16 line 1 to column 17 line 67].

As to claim 9, Ulyanov discloses that the step of decoding the results into output comprises computing X*XUb, external of the host computer, to determine the multiplication of Ub as desired output of the programs wherein XUY* and Yb is (XUb) and X*XUb is obtained by matrix multiplication X*(XUb) [column 26, lines 6-42].

As to claim 10, Ulyanov discloses the step of decoding comprises decrypting at a control computer connected to the network and the host computer [column 26, lines 6-42].

As to claim 11, Ulyanov suggests that the network comprises the Internet [column 16 line 1 to column 17 line 67].

As to claim 12, Ulyanov suggests that the network comprises a virtual private network [column 16 line 1 to column 17 line 67].

As to claim 13, Ulyanov suggests that the network comprises a local area network (LAN) [column 16 line 1 to column 17 line 67].

As to claim 14, Ulyanov discloses embedding one or more constants into the input data string or program, prior to encoding, to detect incorrect execution or data tampering [column 16 line 1 to column 17 line 67].

As to claim 16, Ulyanov discloses that the control computer embeds one or more constants into the unitary matrix or data string, wherein the results from the host computer indicate tampering or incorrect execution of the encoded program [column 16 line 1 to column 17 line 67].

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
May 11, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100